Vulnerability Summary for the Week of December 20, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 12/27/2021 06:29 PM EST

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of December 20, 2021

12/27/2021 06:39 AM EST

Original release date: December 27, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-44179 MISC MISC
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious GIF file.	2021-12-20	9.3	CVE-2021-44180 MISC MISC
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious GIF file.	2021-12-20	9.3	CVE-2021-44181 MISC MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious EXR file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43021 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious PNG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43022 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious EPS/TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43023 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43024 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43025 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43026 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43028 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43029 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	9.3	CVE-2021-43747 MISC
apache -- http_server	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.	2021-12-20	7.5	CVE-2021-44790 MISC MLIST FEDORA CONFIRM
iresturant_project -- iresturant	RCE in Add Review Function in iResturant 1.0 Allows remote attacker to execute commands remotely	2021-12-20	10	CVE-2021-43439 MISC MISC
numpy -- numpy	Incomplete string comparison in the numpy.core component in NumPy1.9.x, which allows attackers to fail the APIs via constructing specific string objects.	2021-12-17	7.5	CVE-2021-34141 MISC
tcman -- gim	TCMAN GIM is vulnerable to a SQL injection vulnerability inside several available webservice methods in /PC/WebService.asmx.	2021-12-17	7.5	CVE-2021-40850 CONFIRM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- audition	Adobe Audition versions 14.4 (and earlier), and 22.0 (and earlier)are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	2021-12-20	4.3	CVE-2021-44698 MISC MISC
adobe -- audition	Adobe Audition versions 14.4 (and earlier), and 22.0 (and earlier)are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	2021-12-20	4.3	CVE-2021-44699 MISC MISC
adobe -- audition	Adobe Audition versions 14.4 (and earlier), and 22.0 (and earlier)are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MOV file.	2021-12-20	4.3	CVE-2021-44697 MISC MISC
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SVG file.	2021-12-20	4.3	CVE-2021-44182 MISC MISC
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.	2021-12-20	4.3	CVE-2021-43763 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- dimension	Adobe Dimension versions 3.4.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.	2021-12-20	4.3	CVE-2021-44183 MISC MISC
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-12-20	4.3	CVE-2021-43748 MISC
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-12-20	4.3	CVE-2021-43749 MISC
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.16 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-12-20	4.3	CVE-2021-43750 MISC
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.16 (and earlier) allows access to an uninitialized pointer vulnerability that allows remote attackers to disclose sensitive information on affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of MP4 files. The issue results from the lack of proper initialization of memory prior to accessing it.	2021-12-20	4.3	CVE-2021-43746 MISC MISC
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.16 (and earlier) allows access to an uninitialized pointer vulnerability that allows remote attackers to disclose sensitive information on affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of MP4 files. The issue results from the lack of proper initialization of memory prior to accessing it.	2021-12-20	4.3	CVE-2021-43030 MISC MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	6.8	CVE-2021-40784 MISC
adobe -- premiere_rush	Adobe Premiere Rush version 1.5.16 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-12-20	6.8	CVE-2021-40783 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'health_filter' parameter.	2021-12-22	4	CVE-2021-21926 MISC
apache -- http_server	A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).	2021-12-20	6.4	CVE-2021-44224 MISC MLIST FEDORA CONFIRM
apache -- log4j	Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0 and 2.12.3.	2021-12-18	5	CVE-2021-45105 MISC CONFIRM MLIST DEBIAN MISC CISCO CONFIRM CERT-VN CONFIRM CONFIRM MLIST FEDORA FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ciphercoin -- contact_form_7_database_addon_-_cfdb7	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in Contact Form 7 Database Addon – CFDB7 WordPress plugin (versions <= 1.2.6.1).	2021-12-22	4.3	CVE-2021-36885 CONFIRM CONFIRM
ciphercoin -- contact_form_7_database_addon_-_cfdb7	Cross-Site Request Forgery (CSRF) vulnerability discovered in Contact Form 7 Database Addon – CFDB7 WordPress plugin (versions <= 1.2.5.9).	2021-12-22	6.8	CVE-2021-36886 CONFIRM MISC
ftpshell -- ftpshell_server	A buffer overflow vulnerability in the Virtual Path Mapping component of FTPShell v6.83 allows attackers to cause a denial of service (DoS).	2021-12-17	5	CVE-2020-18077 MISC
google -- android	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672059.	2021-12-17	4.6	CVE-2021-0899 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672038.	2021-12-17	4.6	CVE-2021-0894 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05670549.	2021-12-17	4.6	CVE-2021-0897 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05671206.	2021-12-17	4.6	CVE-2021-0896 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672003.	2021-12-17	4.6	CVE-2021-0895 MISC
google -- android	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672071.	2021-12-17	4.6	CVE-2021-0898 MISC
google -- android	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05687474.	2021-12-17	4.6	CVE-2021-0893 MISC
google -- android	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05687781.	2021-12-17	4.6	CVE-2021-0679 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05722511.	2021-12-17	4.6	CVE-2021-0678 MISC
google -- android	In Audio Aurisys HAL, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05977326; Issue ID: ALPS05977326.	2021-12-17	4.6	CVE-2021-0673 MISC
google -- android	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05656488.	2021-12-17	4.6	CVE-2021-0903 MISC
google -- android	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05664618.	2021-12-17	4.6	CVE-2021-0901 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 via the lsr_read_anim_values_ex function, which causes a segmentation fault and application crash.	2021-12-22	5	CVE-2021-45266 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iorder_project -- iorder	Multiple Stored XSS Vulnerabilities in the Source Code of iOrder 1.0 allow remote attackers to execute arbitrary code via signup form in the Name and Phone number field.	2021-12-20	4.3	CVE-2021-43440 MISC MISC
laravel -- framework	OS Command injection vulnerability in function link in Filesystem.php in Laravel Framework before 5.8.17.	2021-12-20	6.8	CVE-2020-19316 MISC MISC
livehelperchat -- live_helper_chat	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	2021-12-18	6.8	CVE-2021-4131 CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. It is possible to use action=mcrundo followed by action=mcrrestore to replace the content of any arbitrary page (that the user doesn't have edit rights for). This applies to any public wiki, or a private wiki that has at least one page set in $wgWhitelistRead.	2021-12-17	4	CVE-2021-44857 CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. By using an action=rollback query, attackers can view private wiki contents.	2021-12-17	5	CVE-2021-45038 CONFIRM MISC
mossle -- lemon	A cross-site scripting (XSS) vulnerability in the potrtalItemName parameter in \web\PortalController.java of lemon V1.10.0 allows attackers to execute arbitrary web scripts or HTML.	2021-12-22	4.3	CVE-2020-20597 MISC
mossle -- lemon	A cross-site scripting (XSS) vulnerability in the Editing component of lemon V1.10.0 allows attackers to execute arbitrary web scripts or HTML.	2021-12-22	4.3	CVE-2020-20598 MISC
numpy -- numpy	Null Pointer Dereference vulnerability exists in numpy.sort in NumPy &lt and 1.19 in the PyArray_DescrNew function due to missing return-value validation, which allows attackers to conduct DoS attacks by repetitively creating sort arrays.	2021-12-17	5	CVE-2021-41495 MISC
numpy -- numpy	A Buffer Overflow vulnerability exists in NumPy 1.9.x in the PyArray_NewFromDescr_int function of ctors.c when specifying arrays of large dimensions (over 32) from Python code, which could let a malicious user cause a Denial of Service.	2021-12-17	5	CVE-2021-33430 MISC
open-emr -- openemr	An authenticated SQL injection issue in the calendar search function of OpenEMR 6.0.0 before patch 3 allows an attacker to read data from all tables of the database via the parameter provider_id, as demonstrated by the /interface/main/calendar/index.php?module=PostCalendar&func=search URI.	2021-12-17	6.8	CVE-2021-41843 MISC MISC MISC FULLDISC
opms_project -- opms	A cross-site request forgery (CSRF) in OPMS v1.3 and below allows attackers to arbitrarily add a user account via /user/add.	2021-12-22	4.3	CVE-2020-20595 MISC
personal_blog_cms_project -- personal_blog_cms	Blog CMS v1.0 contains a cross-site scripting (XSS) vulnerability in the /controller/CommentAdminController.java component.	2021-12-22	4.3	CVE-2020-20605 MISC
s-cms -- s-cms	S-CMS Government Station Building System v5.0 contains a cross-site scripting (XSS) vulnerability in /function/booksave.php.	2021-12-22	4.3	CVE-2020-20426 MISC MISC MISC
s-cms -- s-cms	S-CMS Government Station Building System v5.0 contains a cross-site scripting (XSS) vulnerability in the search function.	2021-12-22	4.3	CVE-2020-20425 MISC MISC MISC
salesagility -- suitecrm	SuiteCRM before 7.12.2 and 8.x before 8.0.1 allows authenticated SQL injection.	2021-12-19	6.5	CVE-2021-45041 CONFIRM CONFIRM
sem-cms -- semcms	The checkuser function of SEMCMS 3.8 was discovered to contain a vulnerability which allows attackers to obtain the password in plaintext through a SQL query.	2021-12-17	5	CVE-2020-18081 MISC
sem-cms -- semcms	A vulnerability in /include/web_check.php of SEMCMS v3.8 allows attackers to reset the Administrator account's password.	2021-12-17	5	CVE-2020-18078 MISC
snipeitapp -- snipe-it	snipe-it is vulnerable to Cross-Site Request Forgery (CSRF)	2021-12-18	6.8	CVE-2021-4130 CONFIRM MISC
tcman -- gim	TCMAN GIM is affected by an open redirect vulnerability. This vulnerability allows the redirection of user navigation to pages controlled by the attacker. The exploitation of this vulnerability might allow a remote attacker to obtain information.	2021-12-17	5.8	CVE-2021-40852 CONFIRM
tcman -- gim	TCMAN GIM is vulnerable to a lack of authorization in all available webservice methods listed in /PC/WebService.asmx. The exploitation of this vulnerability might allow a remote attacker to obtain information.	2021-12-17	5	CVE-2021-40851 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tcman -- gim	TCMAN GIM does not perform an authorization check when trying to access determined resources. A remote attacker could exploit this vulnerability to access URL that require privileges without having them. The exploitation of this vulnerability might allow a remote attacker to obtain sensible information.	2021-12-17	6.4	CVE-2021-40853 CONFIRM
vmware -- workspace_one_uem_console	VMware Workspace ONE UEM console 20.0.8 prior to 20.0.8.37, 20.11.0 prior to 20.11.0.40, 21.2.0 prior to 21.2.0.27, and 21.5.0 prior to 21.5.0.37 contain an SSRF vulnerability. This issue may allow a malicious actor with network access to UEM to send their requests without authentication and to gain access to sensitive information.	2021-12-17	5	CVE-2021-22054 MISC
wechat-php-sdk_project -- wechat-php-sdk	Wechat-php-sdk v1.10.2 is affected by a Cross Site Scripting (XSS) vulnerability in Wechat.php.	2021-12-17	4.3	CVE-2021-43678 MISC MISC
wolterskluwer -- teammate_audit_management	Wolters Kluwer TeamMate AM 12.4 Update 1 mishandles attachment uploads, such that an authenticated user may download and execute malicious files.	2021-12-17	6.8	CVE-2021-44035 MISC MISC
x.org -- x_server	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcXFixesCreatePointerBarrier function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-12-17	4.6	CVE-2021-4009 MISC MISC FEDORA FEDORA MISC DEBIAN
x.org -- x_server	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SwapCreateRegister function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-12-17	4.6	CVE-2021-4011 MISC MISC FEDORA FEDORA MISC DEBIAN
x.org -- x_server	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcScreenSaverSuspend function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-12-17	4.6	CVE-2021-4010 MISC MISC FEDORA FEDORA MISC DEBIAN
x.org -- x_server	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcRenderCompositeGlyphs function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-12-17	4.6	CVE-2021-4008 MISC MISC FEDORA FEDORA MISC DEBIAN

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
convos -- convos	A Stored Cross Site Scripting (XSS) issue exists in Convos-Chat before 6.32.	2021-12-17	3.5	CVE-2021-42584 MISC MISC MISC
google -- android	In alac decoder, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06064258; Issue ID: ALPS06064237.	2021-12-17	2.1	CVE-2021-0674 MISC
google -- android	In geniezone driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863009; Issue ID: ALPS05863009.	2021-12-17	2.1	CVE-2021-0676 MISC
google -- android	In ccu driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827154; Issue ID: ALPS05827154.	2021-12-17	2.1	CVE-2021-0677 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672055.	2021-12-17	2.1	CVE-2021-0900 MISC
google -- android	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05656484.	2021-12-17	2.1	CVE-2021-0902 MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0, 19.0, 20,0 and 21.0 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209165.	2021-12-17	3.5	CVE-2021-38883 CONFIRM XF
ibm -- cloud_pak_for_automation	IBM Cloud Pak for Automation 21.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 212357.	2021-12-21	3.5	CVE-2021-38966 XF CONFIRM
iresturant_project -- iresturant	Stored XSS in Signup Form in iResturant 1.0 Allows Remote Attacker to Inject Arbitrary code via NAME and ADDRESS field	2021-12-20	3.5	CVE-2021-43438 MISC MISC
livehelperchat -- live_helper_chat	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-17	3.5	CVE-2021-4132 CONFIRM MISC
mattermost -- mattermost_server	Mattermost 6.0 and earlier fails to sufficiently validate parameters during post creation, which allows authenticated attackers to cause a client-side crash of the web application via a maliciously crafted post.	2021-12-17	3.5	CVE-2021-37863 MISC MISC
metinfo -- metinfo	MetInfo 7.0 beta contains a stored cross-site scripting (XSS) vulnerability in the $name parameter of admin/?n=column&c=index&a=doAddColumn.	2021-12-22	3.5	CVE-2020-20600 MISC
tarteaucitron.js_-_cookies_legislation_amp;_gdpr_project -- tarteaucitron.js_-_cookies_legislation_ amp;_gdpr	Multiple Stored Authenticated Cross-Site Scripting (XSS) vulnerabilities were discovered in tarteaucitron.js – Cookies legislation & GDPR WordPress plugin (versions <= 1.6).	2021-12-20	3.5	CVE-2021-36889 MISC CONFIRM

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
requarks -- wiki.js	Wiki.js is a wiki app built on Node.js. Wiki.js versions 2.5.257 and earlier are vulnerable to stored cross-site scripting through a SVG file upload. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `<img>` tags. Commit 5d3e81496fba1f0fbd64eeb855f30f69a9040718 fixes this vulnerability by adding an optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users. Wiki.js version 2.5.260 is the first production version to contain a patch. Version 2.5.258 is the first development build to contain a patch and is available only as a Docker image as requarks/wiki:canary-2.5.258.	2021-12-20	not yet calculated	CVE-2021-43842 MISC MISC CONFIRM
4mosan_gcb_doctor -- 4mosan_gcb_doctor	4MOSAn GCB Doctor's file upload function has improper user privilege control. A remote attacker can upload arbitrary files including webshell files without authentication and execute arbitrary code in order to perform arbitrary system operations or deny of service attack.	2021-12-20	not yet calculated	CVE-2021-44159 CONFIRM
abode_iota -- all-in-one_security_kit	OS Command Injection vulnerability in the wirelessConnect handler of Abode iota All-In-One Security Kit allows an attacker to inject commands and gain root access. This issue affects: Abode iota All-In-One Security Kit versions prior to 1.0.2.23_6.9V_dev_t2_homekit_RF_2.0.19_s2_kvsABODE oz.	2021-12-20	not yet calculated	CVE-2020-8105 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acclaim -- usaherds	Acclaim USAHERDS through 7.4.0.1 uses hard-coded credentials.	2021-12-21	not yet calculated	CVE-2021-44207 MISC MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'mac_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21928 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'host_alt_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21937 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'health_alt_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21936 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'host_alt_filter2' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21935 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'imei_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21934 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'esn_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21933 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'name_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21932 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at' stat_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21931 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'username_filter' parameter with the administrative account or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21922 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'prod_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21929 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'name_filter' parameter with the administrative account or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21921 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'loc_filter' parameter.	2021-12-22	not yet calculated	CVE-2021-21927 MISC
advantech -- r-seenet	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'description_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21916 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'surname_filter' parameter with the administrative account or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21920 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ord' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.	2021-12-22	not yet calculated	CVE-2021-21919 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'name_filter' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.	2021-12-22	not yet calculated	CVE-2021-21918 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'firm_filter' parameter.	2021-12-22	not yet calculated	CVE-2021-21925 MISC
advantech -- r-seenet	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at ''ord' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21917 MISC
advantech -- r-seenet	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'company_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21915 MISC
advantech -- r-seenet	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21912 MISC
advantech -- r-seenet	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21911 MISC
advantech -- r-seenet	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21910 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'company_filter' parameter with the administrative account or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21923 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'desc_filter' parameter.	2021-12-22	not yet calculated	CVE-2021-21924 MISC
advantech -- r-seenet	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'sn_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	2021-12-22	not yet calculated	CVE-2021-21930 MISC
ajax -- ajax.net_professional	Ajax.NET Professional (AjaxPro) is an AJAX framework available for Microsoft ASP.NET. Affected versions of this package are vulnerable to JavaScript object injection which may result in cross site scripting when leveraged by a malicious user. The affected core relates to JavaScript object creation when parsing json input. Releases before version 21.12.22.1 are affected. A workaround exists that replaces one of the core JavaScript files embedded in the library. See the GHSA-5q7q-qqw2-hjq7 for workaround details.	2021-12-22	not yet calculated	CVE-2021-43853 CONFIRM MISC MISC
anker_eufy -- homeba	An authentication bypass vulnerability exists in the process_msg() function of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted man-in-the-middle attack can lead to increased privileges.	2021-12-22	not yet calculated	CVE-2021-21953 MISC
anker_eufy -- homebase	An authentication bypass vulnerability exists in the CMD_DEVICE_GET_RSA_KEY_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to increased privileges.	2021-12-22	not yet calculated	CVE-2021-21952 MISC
anuko -- time_tracker	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. SQL injection vulnerability exist in multiple files in Time Tracker version 1.19.33.5606 and prior due to not properly checking of the "group" and "status" parameters in POST requests. Group parameter is posted along when navigating between organizational subgroups (groups.php file). Status parameter is used in multiple files to change a status of an entity such as making a project, task, or user inactive. This issue has been patched in version 1.19.33.5607. An upgrade is highly recommended. If an upgrade is not practical, introduce ttValidStatus function as in the latest version and start using it user input check blocks wherever status field is used. For groups.php fix, introduce ttValidInteger function as in the latest version and use it in the access check block in the file.	2021-12-22	not yet calculated	CVE-2021-43851 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- cordova	cordova-plugin-fingerprint-aio is a plugin provides a single and simple interface for accessing fingerprint APIs on both Android 6+ and iOS. In versions prior to 5.0.1 The exported activity `de.niklasmerz.cordova.biometric.BiometricActivity` can cause the app to crash. This vulnerability occurred because the activity didn't handle the case where it is requested with invalid or empty data which results in a crash. Any third party app can constantly call this activity with no permission. A 3rd party app/attacker using event listener can continually stop the app from working and make the victim unable to open it. Version 5.0.1 of the cordova-plugin-fingerprint-aio doesn't export the activity anymore and is no longer vulnerable. If you want to fix older versions change the attribute android:exported in plugin.xml to false. Please upgrade to version 5.0.1 as soon as possible.	2021-12-23	not yet calculated	CVE-2021-43849 CONFIRM MISC MISC
apache -- parquet	Improper Input Validation vulnerability in Parquet-MR of Apache Parquet allows an attacker to DoS by malicious Parquet files. This issue affects Apache Parquet-MR version 1.9.0 and later versions.	2021-12-20	not yet calculated	CVE-2021-41561 MISC MLIST
apache -- plc	Apache PLC4X - PLC4C (Only the C language implementation was effected) was vulnerable to an unsigned integer underflow flaw inside the tcp transport. Users should update to 0.9.1, which addresses this issue. However, in order to exploit this vulnerability, a user would have to actively connect to a mallicious device which could send a response with invalid content. Currently we consider the probability of this being exploited as quite minimal, however this could change in the future, especially with the industrial networks growing more and more together.	2021-12-19	not yet calculated	CVE-2021-43083 MISC MLIST
apache -- solr	An Improper Input Validation vulnerability in DataImportHandler of Apache Solr allows an attacker to provide a Windows UNC path resulting in an SMB network call being made from the Solr host to another host on the network. If the attacker has wider access to the network, this may lead to SMB attacks, which may result in: * The exfiltration of sensitive data such as OS user hashes (NTLM/LM hashes), * In case of misconfigured systems, SMB Relay Attacks which can lead to user impersonation on SMB Shares or, in a worse-case scenario, Remote Code Execution This issue affects all Apache Solr versions prior to 8.11.1. This issue only affects Windows.	2021-12-23	not yet calculated	CVE-2021-44548 MISC
apple -- ios	An issue existed in preventing the uploading of CallKit call history to iCloud. This issue was addressed through improved logic. This issue is fixed in iOS 10.2.1. Updates for CallKit call history are sent to iCloud.	2021-12-23	not yet calculated	CVE-2017-2375 MISC
apple -- ios_and_watchos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 11.2, watchOS 4.2. An application may be able to execute arbitrary code with kernel privilege.	2021-12-23	not yet calculated	CVE-2017-13880 MISC MISC
apple -- macos_high_sierra	A validation issue was addressed with improved logic. This issue is fixed in macOS High Sierra 10.13.5, Security Update 2018-003 Sierra, Security Update 2018-003 El Capitan. An attacker with physical access to a device may be able to elevate privileges.	2021-12-23	not yet calculated	CVE-2018-4478 MISC
apple -- macos_high_sierra	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS High Sierra 10.13. An application may be able to execute arbitrary code with elevated privileges.	2021-12-23	not yet calculated	CVE-2017-13835 MISC
apple -- macos_high_sierra	An issue existed in the handling of Contact sharing. This issue was addressed with improved handling of user information. This issue is fixed in macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan. Sharing contact information may lead to unexpected data sharing.	2021-12-23	not yet calculated	CVE-2017-13892 MISC
apple -- macos_mojave	CVE-2019-8643: Arun Sharma of VMWare This issue is fixed in macOS Mojave 10.14. Description: A logic issue was addressed with improved state management..	2021-12-23	not yet calculated	CVE-2019-8643 MISC
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. A malicious application may be able to execute arbitrary code with kernel privileges.	2021-12-23	not yet calculated	CVE-2020-3886 MISC
apple -- multiple_products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. A malicious application may be able to overwrite arbitrary files.	2021-12-23	not yet calculated	CVE-2020-3896 MISC
apple -- multiple_products	This issue was addressed with a new entitlement. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra, iOS 12.4, tvOS 12.4. A local user may be able to read a persistent account identifier.	2021-12-23	not yet calculated	CVE-2019-8702 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed with improved entitlements. This issue is fixed in watchOS 6, tvOS 13, macOS Catalina 10.15, iOS 13. An application may be able to gain elevated privileges.	2021-12-23	not yet calculated	CVE-2019-8703 MISC MISC MISC MISC
apple -- multiple_products	A null pointer dereference was addressed with improved validation. This issue is fixed in macOS High Sierra 10.13, iCloud for Windows 7.0, watchOS 4, iOS 11, iTunes 12.7 for Windows. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution.	2021-12-23	not yet calculated	CVE-2018-4302 MISC MISC MISC MISC MISC
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.2, macOS Monterey 12.1, Security Update 2021-008 Catalina, iOS 15.2 and iPadOS 15.2, watchOS 8.3. A local user may be able to modify protected parts of the file system.	2021-12-23	not yet calculated	CVE-2021-30767 MISC MISC MISC MISC MISC
apple -- remote_desktop	A cryptographic weakness existed in the authentication protocol of Remote Desktop. This issue was addressed by implementing the Secure Remote Password authentication protocol. This issue is fixed in Apple Remote Desktop 3.9. An attacker may be able to capture cleartext passwords.	2021-12-23	not yet calculated	CVE-2017-2488 MISC
apple --multiple_products	A race condition was addressed with additional validation. This issue is fixed in tvOS 11.2, iOS 11.2, macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan, watchOS 4.2. An application may be able to gain elevated privileges.	2021-12-23	not yet calculated	CVE-2017-13905 MISC MISC MISC MISC
apple -- macos_high_sierra	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, macOS High Sierra 10.13. A malicious application may be able to elevate privileges.	2021-12-23	not yet calculated	CVE-2017-13906 MISC MISC
apple -- macos_high_sierra	An issue in handling file permissions was addressed with improved validation. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, macOS High Sierra 10.13. A local attacker may be able to execute non-executable text files via an SMB share.	2021-12-23	not yet calculated	CVE-2017-13908 MISC MISC
apple -- macos_high_sierra	An issue existed in the storage of sensitive tokens. This issue was addressed by placing the tokens in Keychain. This issue is fixed in macOS High Sierra 10.13. A local attacker may gain access to iCloud authentication tokens.	2021-12-23	not yet calculated	CVE-2017-13909 MISC
apple -- macos_high_sierra	An access issue was addressed with additional sandbox restrictions on applications. This issue is fixed in macOS High Sierra 10.13. An application may be able to access restricted files.	2021-12-23	not yet calculated	CVE-2017-13910 MISC
apple -- macos_high_sierra	A state management issue was addressed with improved state validation. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan. The screen lock may unexpectedly remain unlocked.	2021-12-23	not yet calculated	CVE-2017-13907 MISC
archivy -- archivy	archivy is vulnerable to Cross-Site Request Forgery (CSRF)	2021-12-25	not yet calculated	CVE-2021-4162 CONFIRM MISC
armmbed -- mbed_tls	In Mbed TLS before 3.1.0, psa_aead_generate_nonce allows policy bypass or oracle-based decryption when the output buffer is at memory locations accessible to an untrusted application.	2021-12-21	not yet calculated	CVE-2021-45451 MISC
armmbed -- mbed_tls	In Mbed TLS before 2.28.0 and 3.x before 3.1.0, psa_cipher_generate_iv and psa_cipher_encrypt allow policy bypass or oracle-based decryption when the output buffer is at memory locations accessible to an untrusted application.	2021-12-21	not yet calculated	CVE-2021-45450 MISC MISC
armmbed -- mbed_tls	Mbed TLS before 3.0.1 has a double free in certain out-of-memory conditions, as demonstrated by an mbedtls_ssl_set_session() failure.	2021-12-20	not yet calculated	CVE-2021-44732 CONFIRM MISC CONFIRM CONFIRM CONFIRM CONFIRM
autodesk -- pdftron	A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files through PDF earlier than 9.0.7 version.	2021-12-23	not yet calculated	CVE-2021-40161 MISC
autodesk -- pdftron	A maliciously crafted PDF file prior to 9.0.7 may be forced to read beyond allocated boundaries when parsing the PDF file. This vulnerability can be exploited to execute arbitrary code.	2021-12-23	not yet calculated	CVE-2021-40160 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
blackmagic_design -- davinci_resolve	When parsing a file that is submitted to the DPDecoder service as a job, the R3D SDK will mistakenly skip over the assignment of a property containing an object referring to a UUID that was parsed from a frame within the video container. Upon destruction of the object that owns it, the uninitialized member will be dereferenced and then destroyed using the object's virtual destructor. Due to the object property being uninitialized, this can result in dereferencing an arbitrary pointer for the object's virtual method table, which can result in code execution under the context of the application.	2021-12-22	not yet calculated	CVE-2021-40418 MISC
blackmagic_design -- davinci_resolve	When parsing a file that is submitted to the DPDecoder service as a job, the service will use the combination of decoding parameters that were submitted with the job along with fields that were parsed for the submitted video by the R3D SDK to calculate the size of a heap buffer. Due to an integer overflow with regards to this calculation, this can result in an undersized heap buffer being allocated. When this heap buffer is written to, a heap-based buffer overflow will occur. This can result in code execution under the context of the application.	2021-12-22	not yet calculated	CVE-2021-40417 MISC
chain_sea_ -- ai_chatbot_system	Chain Sea ai chatbot backend has improper filtering of special characters in URL parameters, which allows a remote attacker to perform JavaScript injection for XSS (reflected Cross-site scripting) attack without authentication.	2021-12-20	not yet calculated	CVE-2021-44163 CONFIRM
chain_sea_ -- ai_chatbot_system	Chain Sea ai chatbot system's file upload function has insufficient filtering for special characters in URLs, which allows a remote attacker to by-pass file type validation, upload malicious script and execute arbitrary code without authentication, in order to take control of the system or terminate service.	2021-12-20	not yet calculated	CVE-2021-44164 CONFIRM
chain_sea_ -- ai_chatbot_system	Chain Sea ai chatbot system's specific file download function has path traversal vulnerability. The function has improper filtering of special characters in URL parameters, which allows a remote attacker to download arbitrary system files without authentication.	2021-12-20	not yet calculated	CVE-2021-44162 CONFIRM
crypto-org-chain -- cronos	Cronos is a commercial implementation of a blockchain. In Cronos nodes running versions before v0.6.5, it is possible to take transaction fees from Cosmos SDK's FeeCollector for the current block by sending a custom crafted MsgEthereumTx. This problem has been patched in Cronos v0.6.5. There are no tested workarounds. All validator node operators are recommended to upgrade to Cronos v0.6.5 at their earliest possible convenience.	2021-12-21	not yet calculated	CVE-2021-43839 MISC CONFIRM MISC
cve-search -- cve-search	lib/DatabaseLayer.py in cve-search before 4.1.0 allows regular expression injection, which can lead to ReDoS (regular expression denial of service) or other impacts.	2021-12-23	not yet calculated	CVE-2021-45470 MISC MISC MISC
dalmark -- system_systeams	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to Insecure design on report build via SQL query. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. The bi report module exposes direct SQL commands via POST data in order to select data for report generation. A malicious actor can use the bi report endpoint as a direct SQL prompt under the authenticated user.	2021-12-21	not yet calculated	CVE-2021-44874 MISC
dalmark -- system_systeams	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to User enumeration. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. This issue occurs during the password recovery procedure for a given user, where a difference in messages could allow an attacker to determine if the given user is valid or not, enabling a brute force attack with valid users.	2021-12-21	not yet calculated	CVE-2021-44875 MISC
dalmark -- system_systeams	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to User enumeration. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. This issue occurs during the identification of the correct tenant for a given user, where a difference in messages could allow an attacker to determine if the given user is valid or not, enabling a brute force attack with valid users.	2021-12-21	not yet calculated	CVE-2021-44876 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dalmark -- system_systeams	Dalmark Systems Systeam 2.22.8 build 1724 is vulnerable to Incorrect Access Control. The Systeam application is an ERP system that uses a mixed architecture based on SaaS tenant and user management, and on-premise database and web application counterparts. A broken access control vulnerability has been found while using a temporary generated token in order to consume api resources. The vulnerability allows an unauthenticated attacker to use an api endpoint to generate a temporary JWT token that is designed to reference the correct tenant prior to authentication, to request system configuration parameters using direct api requests. The correct exploitation of this vulnerability causes sensitive information exposure. In case the tenant has an smtp credential set, the full credential information is disclosed.	2021-12-21	not yet calculated	CVE-2021-44877 MISC
dell -- emc_avamar_server	Dell EMC Avamar Server versions 18.2, 19.1, 19.2, 19.3, and 19.4 contain an improper privilege management vulnerability in AUI. A malicious user with high privileges could potentially exploit this vulnerability, leading to the disclosure of the AUI info and performing some unauthorized operation on the AUI.	2021-12-21	not yet calculated	CVE-2021-36316 CONFIRM
dell -- emc_avamar_server	Dell EMC Avamar Server version 19.4 contains a plain-text password storage vulnerability in AvInstaller. A local attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2021-12-21	not yet calculated	CVE-2021-36317 CONFIRM
dell -- emc_avamar_server	Dell EMC Avamar versions 18.2,19.1,19.2,19.3,19.4 contain a plain-text password storage vulnerability. A high privileged user could potentially exploit this vulnerability, leading to a complete outage.	2021-12-21	not yet calculated	CVE-2021-36318 CONFIRM
dell -- powerpath_management_applicance	Dell PowerPath Management Appliance, versions 3.2, 3.1, 3.0 P01, 3.0, and 2.6, use hard-coded cryptographic key. A local high-privileged malicious user may potentially exploit this vulnerability to gain access to secrets and elevate to gain higher privileges.	2021-12-21	not yet calculated	CVE-2021-43587 CONFIRM
dell -- powerscale_onefs	Dell PowerScale OneFS, versions 8.2.2-9.3.0.x, contain an authentication bypass by primary weakness in one of the authentication factors. A remote unauthenticated attacker may potentially exploit this vulnerability and bypass one of the factors of authentication.	2021-12-21	not yet calculated	CVE-2021-36350 CONFIRM
dell -- wyse_device_agent	Dell Wyse Device Agent version 14.5.4.1 and below contain a sensitive data exposure vulnerability. A local authenticated user with low privileges could potentially exploit this vulnerability in order to access sensitive information.	2021-12-21	not yet calculated	CVE-2021-36341 CONFIRM
dell -- wyse_management_suite	Dell Wyse Management Suite version 3.3.1 and prior support insecure Transport Security Protocols TLS 1.0 and TLS 1.1 which are susceptible to Man-In-The-Middle attacks thereby compromising Confidentiality and Integrity of data.	2021-12-21	not yet calculated	CVE-2021-36337 CONFIRM
dell -- wyse_management_suite	Wyse Management Suite 3.3.1 and below versions contain a deserialization vulnerability that could allow an unauthenticated attacker to execute code on the affected system.	2021-12-21	not yet calculated	CVE-2021-36336 CONFIRM
delta_electronics -- diaenergie	DIAEnergie Version 1.7.5 and prior is vulnerable to multiple cross-site scripting vulnerabilities when arbitrary code is injected into the parameter “name” of the script “HandlerEnergyType.ashx”.	2021-12-22	not yet calculated	CVE-2021-44544 MISC
delta_electronics -- diaenergie	DIAEnergie Version 1.7.5 and prior is vulnerable to stored cross-site scripting when an unauthenticated user injects arbitrary code into the parameter “descr” of the script “DIAE_hierarchyHandler.ashx”.	2021-12-22	not yet calculated	CVE-2021-31558 MISC
delta_electronics -- diaenergie	DIAEnergie Version 1.7.5 and prior is vulnerable to stored cross-site scripting when an unauthenticated user injects arbitrary code into the parameter “name” of the script “DIAE_HandlerAlarmGroup.ashx”.	2021-12-22	not yet calculated	CVE-2021-44471 MISC
delta_electronics -- diaenergie	DIAEnergie Version 1.7.5 and prior is vulnerable to a reflected cross-site scripting attack through error pages that are returned by “.NET Request.QueryString”.	2021-12-22	not yet calculated	CVE-2021-23228 MISC
e2guardian -- e2guardian	e2guardian v5.4.x <= v5.4.3r is affected by missing SSL certificate validation in the SSL MITM engine. In standalone mode (i.e., acting as a proxy or a transparent proxy), with SSL MITM enabled, e2guardian, if built with OpenSSL v1.1.x, did not validate hostnames in certificates of the web servers that it connected to, and thus was itself vulnerable to MITM attacks.	2021-12-23	not yet calculated	CVE-2021-44273 MISC MISC MLIST
eap -- eap	The HornetQ component of Artemis in EAP 7 was not updated with the fix for CVE-2016-4978. A remote attacker could use this flaw to execute arbitrary code with the permissions of the application using a JMS ObjectMessage.	2021-12-23	not yet calculated	CVE-2021-20318 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elgg -- elgg	elgg is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-24	not yet calculated	CVE-2021-4072 MISC CONFIRM
enc_security -- deltavault	ENC DataVault 7.1.1W and VaultAPI v67, which is currently being used in various other applications, mishandles key derivation, making it easier for attackers to determine the passwords of all DataVault users (across USB drives sold under multiple brand names).	2021-12-22	not yet calculated	CVE-2021-36750 MISC MISC
f-secure -- antivirus_engine	A vulnerability affecting F-Secure antivirus engine was discovered whereby scanning MS outlook .pst files can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine.	2021-12-22	not yet calculated	CVE-2021-40836 MISC
freepbx -- freepbx	FreePBX, when restapps (aka Rest Phone Apps) 15.0.19.87, 15.0.19.88, 16.0.18.40, or 16.0.18.41 is installed, allows remote attackers to execute arbitrary code, as exploited in the wild in December 2021. The fixed versions are 15.0.20 and 16.0.19.	2021-12-22	not yet calculated	CVE-2021-45461 CONFIRM CONFIRM MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an access of uninitialized pointer, which may allow an attacker read from or write to unexpected memory locations, leading to a denial-of-service.	2021-12-20	not yet calculated	CVE-2021-38409 MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to a stack-based buffer overflow, which may allow an attacker to achieve code execution.	2021-12-20	not yet calculated	CVE-2021-38413 MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an untrusted pointer dereference, which may allow an attacker to execute arbitrary code and cause the application to crash.	2021-12-20	not yet calculated	CVE-2021-38401 MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable a heap-based buffer overflow when parsing a specially crafted project file, which may allow an attacker to execute arbitrary code.	2021-12-20	not yet calculated	CVE-2021-38415 MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds write, which can result in data corruption, a system crash, or code execution.	2021-12-20	not yet calculated	CVE-2021-38419 MISC
fuji_electric -- v-server_lite_and_tellus_lite_v-simulator	Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds read, which may allow an attacker to read sensitive information from other memory locations or cause a crash.	2021-12-20	not yet calculated	CVE-2021-38421 MISC
garrett -- metal_detectors	Specially-crafted command line arguments can lead to arbitrary file deletion. The handle_delete function does not attempt to sanitize or otherwise validate the contents of the [file] parameter (passed to the function as argv[1]), allowing an authenticated attacker to supply directory traversal primitives and delete semi-arbitrary files.	2021-12-22	not yet calculated	CVE-2021-21908 MISC
garrett -- metal_detectors	Specially-crafted command line arguments can lead to arbitrary file deletion in the del .cnt|.log file delete command. An attacker can provide malicious inputs to trigger this vulnerability	2021-12-22	not yet calculated	CVE-2021-21909 MISC
garrett -- metal_detectors	A directory traversal vulnerability exists in the CMA CLI getenv command functionality of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted command line argument can lead to local file inclusion. An attacker can provide malicious input to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21907 MISC
garrett -- metal_detectors	Stack-based buffer overflow vulnerability exists in how the CMA readfile function of Garrett Metal Detectors iC Module CMA Version 5.0 is used at various locations. The Garrett iC Module exposes an authenticated CLI over TCP port 6877. This interface is used by a secondary GUI client, called "CMA Connect", to interact with the iC Module on behalf of the user. Every time a user submits a password to the CLI password prompt, the buffer containing their input is passed as the password parameter to the checkPassword function.	2021-12-22	not yet calculated	CVE-2021-21906 MISC
garrett -- metal_detectors	Stack-based buffer overflow vulnerability exists in how the CMA readfile function of Garrett Metal Detectors iC Module CMA Version 5.0 is used at various locations. The Garrett iC Module exposes an authenticated CLI over TCP port 6877. This interface is used by a secondary GUI client, called "CMA Connect", to interact with the iC Module on behalf of the user. After a client successfully authenticates, they can send plaintext commands to manipulate the device.	2021-12-22	not yet calculated	CVE-2021-21905 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
garrett -- metal_detectors	A directory traversal vulnerability exists in the CMA CLI setenv command of Garrett Metal Detectors' iC Module CMA Version 5.0. An attacker can provide malicious input to trigger this vulnerability	2021-12-22	not yet calculated	CVE-2021-21904 MISC
garrett -- metal_detectors	A stack-based buffer overflow vulnerability exists in the CMA check_udp_crc function of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted packet can lead to a stack-based buffer overflow during a call to strcpy. An attacker can send a malicious packet to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21903 MISC
garrett -- metal_detectors	An authentication bypass vulnerability exists in the CMA run_server_6877 functionality of Garrett Metal Detectors iC Module CMA Version 5.0. A properly-timed network connection can lead to authentication bypass via session hijacking. An attacker can send a sequence of requests to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21902 MISC
garrett -- metal_detectors	A stack-based buffer overflow vulnerability exists in the CMA check_udp_crc function of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted packet can lead to a stack-based buffer overflow during a call to memcpy. An attacker can send a malicious packet to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21901 MISC
gerbv_project -- gerbv	An out-of-bounds write vulnerability exists in the RS-274X aperture macro variables handling functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and the forked version of Gerbv (commit 71493260). A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-40394 MISC
gerbv_project -- gerbv	An out-of-bounds write vulnerability exists in the RS-274X aperture macro variables handling functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and the forked version of Gerbv (commit 71493260). A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-40393 MISC
gnome -- gimp	GEGL before 0.4.34, as used (for example) in GIMP before 2.10.30, allows shell expansion when a pathname in a constructed command line is not escaped or filtered. This is caused by use of the system library function for execution of the ImageMagick convert fallback in magick-load.	2021-12-23	not yet calculated	CVE-2021-45463 MISC MISC MISC MISC
gnu -- gnu	An Invalid Pointer vulnerability exists in GNU patch 2.7 via the another_hunk function, which causes a Denial of Service.	2021-12-22	not yet calculated	CVE-2021-45261 MISC
gnuplot -- gnuplot	A Divide by Zero vulnerability exists in gnuplot 5.4 in the boundary3d function in graph3d.c, which could cause a Arithmetic exception and application crash.	2021-12-21	not yet calculated	CVE-2021-44917 MISC
go -- gocd_server	Adding a new pipeline in GoCD server version 21.3.0 has a functionality that could be abused to do an un-intended action in order to achieve a Server Side Request Forgery (SSRF)	2021-12-22	not yet calculated	CVE-2021-44659 MISC MISC MISC MISC
google -- chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38019 MISC MISC
google -- chrome	Insufficient policy enforcement in contacts picker in Google Chrome on Android prior to 96.0.4664.45 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38020 MISC MISC
google -- chrome	Inappropriate implementation in navigation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38018 MISC MISC
google -- chrome	Inappropriate implementation in WebAuthentication in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38022 MISC MISC
google -- chrome	Insufficient policy enforcement in iframe sandbox in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38017 MISC MISC
google -- chrome	Insufficient policy enforcement in background fetch in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38016 MISC MISC
google -- chrome	Inappropriate implementation in input in Google Chrome prior to 96.0.4664.45 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2021-12-23	not yet calculated	CVE-2021-38015 MISC MISC
google -- chrome	Out of bounds write in Swiftshader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38014 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in referrer in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38021 MISC MISC
google -- chrome	Insufficient data validation in new tab page in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4068 MISC MISC
google -- chrome	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38011 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4061 MISC MISC
google -- chrome	Use after free in window manager in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4067 MISC MISC
google -- chrome	Integer underflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4066 MISC MISC
google -- chrome	Use after free in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4065 MISC MISC
google -- chrome	Use after free in screen capture in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4064 MISC MISC
google -- chrome	Use after free in developer tools in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4063 MISC MISC
google -- chrome	Heap buffer overflow in BFCache in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4062 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4078 MISC MISC
google -- chrome	Insufficient data validation in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4059 MISC MISC
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via crafted WebRTC packets.	2021-12-23	not yet calculated	CVE-2021-4079 MISC MISC
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4058 MISC MISC
google -- chrome	Use after free in file API in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4057 MISC MISC
google -- chrome	Type confusion in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4056 MISC MISC
google -- chrome	Heap buffer overflow in extensions in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	2021-12-23	not yet calculated	CVE-2021-4055 MISC MISC
google -- chrome	Incorrect security UI in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4054 MISC MISC
google -- chrome	Use after free in UI in Google Chrome on Linux prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-4053 MISC MISC
google -- chrome	Use after free in web apps in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	2021-12-23	not yet calculated	CVE-2021-4052 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38012 MISC MISC
google -- chrome	Heap buffer overflow in fingerprint recognition in Google Chrome on ChromeOS prior to 96.0.4664.45 allowed a remote attacker who had compromised a WebUI renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38013 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in service workers in Google Chrome prior to 96.0.4664.45 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38010 MISC MISC
google -- chrome	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38006 MISC MISC
google -- chrome	Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38005 MISC MISC
google -- chrome	Inappropriate implementation in cache in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38009 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38007 MISC MISC
google -- chrome	Use after free in media in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-12-23	not yet calculated	CVE-2021-38008 MISC MISC
gpac -- gpac	An infinite loop vulnerability exists in gpac 1.1.0 in the gf_log function, which causes a Denial of Service.	2021-12-21	not yet calculated	CVE-2021-44924 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_svg_get_attribute_name function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44925 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_isom_parse_movie_boxes_internal function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44921 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the lsr_read_id.part function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45260 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_sg_vrml_mf_append function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44927 MISC
gpac -- gpac	An infinite loop vulnerability exists in Gpac 1.0.1 in gf_get_bit_size.	2021-12-21	not yet calculated	CVE-2021-45297 MISC
gpac -- gpac	The gf_isom_hint_rtp_read function in GPAC 1.0.1 allows attackers to cause a denial of service (Invalid memory address dereference) via a crafted file in the MP4Box command.	2021-12-21	not yet calculated	CVE-2021-45292 MISC
gpac -- gpac	The gf_dump_setup function in GPAC 1.0.1 allows malicoius users to cause a denial of service (Invalid memory address dereference) via a crafted file in the MP4Box command.	2021-12-21	not yet calculated	CVE-2021-45291 MISC
gpac -- gpac	An invalid free vulnerability exists in gpac 1.1.0 via the gf_sg_command_del function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45262 MISC
gpac -- gpac	A vulnerability exists in GPAC 1.0.1 due to an omission of security-relevant Information, which could cause a Denial of Service. The program terminates with signal SIGKILL.	2021-12-21	not yet calculated	CVE-2021-45289 MISC
gpac -- gpac	A Double Free vulnerability exists in filedump.c in GPAC 1.0.1, which could cause a Denail of Service via a crafted file in the MP4Box command.	2021-12-21	not yet calculated	CVE-2021-45288 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in the gpac in the gf_node_get_tag function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44926 MISC
gpac -- gpac	An invalid memory address dereference vulnerability exists in gpac 1.1.0 in the dump_od_to_saf.isra function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44920 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the BD_CheckSFTimeOffset function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44922 MISC
gpac -- gpac	A Null Pointer Dereference vulnerability exists in the gf_sg_vrml_mf_alloc function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44919 MISC
gpac -- gpac	A Null Pointer Dereference vulnerability exists in gpac 1.1.0 in the gf_node_get_field function, which can cause a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44918 MISC
gpac -- gpac	An Invalid pointer reference vulnerability exists in gpac 1.1.0 via the gf_svg_node_del function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45259 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	An invalid free vulnerability exists in gpac 1.1.0 via the gf_svg_delete_attribute_value function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45263 MISC
gpac -- gpac	A null pointer dereference vulnerability exists in gpac 1.1.0 in the gf_dump_vrml_dyn_field.isra function, which causes a segmentation fault and application crash.	2021-12-21	not yet calculated	CVE-2021-44923 MISC
gpac -- gpac	A stack overflow vulnerability exists in gpac 1.1.0 via the gf_bifs_dec_proto_list function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45258 MISC
gpac -- gpac	An invalid memory address dereference vulnerability exists in gpac 1.1.0 via the svg_node_start function, which causes a segmentation fault and application crash.	2021-12-22	not yet calculated	CVE-2021-45267 MISC
groupsession -- multiple_products	Incorrect permission assignment for critical resource vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to access arbitrary files on the server and obtain sensitive information via unspecified vectors.	2021-12-24	not yet calculated	CVE-2021-20874 MISC MISC
groupsession -- multiple_products	Path traversal vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows an attacker with an administrative privilege to obtain sensitive information stored in the hierarchy above the directory on the published site's server via unspecified vectors.	2021-12-24	not yet calculated	CVE-2021-20876 MISC MISC
groupsession -- multiple_products	Open redirect vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary web sites and conduct phishing attacks by having a user to access a specially crafted URL.	2021-12-24	not yet calculated	CVE-2021-20875 MISC MISC
gurock -- testrail	Gurock TestRail before 7.2.4 mishandles HTML escaping.	2021-12-20	not yet calculated	CVE-2021-44263 CONFIRM
hivex -- hivex	A flaw was found in the hivex library. This flaw allows an attacker to input a specially crafted Windows Registry (hive) file, which would cause hivex to recursively call the _get_children() function, leading to a stack overflow. The highest threat from this vulnerability is to system availability.	2021-12-23	not yet calculated	CVE-2021-3622 MISC FEDORA FEDORA MISC MISC
humhub -- humhub	HumHub is an open-source social network kit written in PHP. Prior to HumHub version 1.10.3 or 1.9.3, it could be possible for registered users to become unauthorized members of private Spaces. Versions 1.10.3 and 1.9.3 contain a patch for this issue.	2021-12-20	not yet calculated	CVE-2021-43847 MISC MISC MISC MISC CONFIRM
ibm -- business_process_manager	IBM Business Process Manager 8.5 and 8.6 and IBM Business Automation Workflow 18.0, 19.0, 20.0 and 21.0 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209512.	2021-12-21	not yet calculated	CVE-2021-38893 XF CONFIRM CONFIRM
ibm -- business_process_manager	IBM Business Process Manager 8.5 and 8.6 and IBM Business Automation Workflow 18.0, 19.0, 20.0 and 21.0 could allow a privileged user to obtain highly sensitive information due to improper access controls. IBM X-Force ID: 209607.	2021-12-21	not yet calculated	CVE-2021-38900 CONFIRM CONFIRM XF
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.7.2.0, 1.7.1.0, and 1.7.0.0 could allow an authenticated user to obtain sensitive information in HTTP responses that could be used in further attacks against the system. IBM X-Force ID: 213651.	2021-12-22	not yet calculated	CVE-2021-39013 XF CONFIRM
idec_plcs -- idec_plcs	Plaintext storage of a password vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from file servers, backup repositories, or ZLD files saved in SD cards. As a result, the attacker may access the PLC Web server and hijack the PLC, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	2021-12-24	not yet calculated	CVE-2021-20827 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idec_plcs -- idec_plcs	Unprotected transport of credentials vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from the communication between the PLC and the software. As a result, the complete access privileges to the PLC Web server may be obtained, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	2021-12-24	not yet calculated	CVE-2021-20826 MISC MISC
invoiceninja -- invoiceninja	invoiceninja is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-24	not yet calculated	CVE-2021-3977 MISC CONFIRM
jfrog_artifactory -- jfrog_artifactory	JFrog Artifactory before 7.25.4 (Enterprise+ deployments only), is vulnerable to Blind SQL Injection by a low privileged authenticated user due to incomplete validation when performing an SQL query.	2021-12-20	not yet calculated	CVE-2021-3860 MISC
js-data -- js-data	All versions of package js-data are vulnerable to Prototype Pollution via the deepFillIn and the set functions. This is an incomplete fix of [CVE-2020-28442](https://snyk.io/vuln/SNYK-JS-JSDATA-1023655).	2021-12-24	not yet calculated	CVE-2021-23574 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
jsx-slack -- jsx-slack	jsx-slack is a package for building JSON objects for Slack block kit surfaces from JSX. The maintainers found the patch for CVE-2021-43838 in jsx-slack v4.5.1 is insufficient tfor protection from a Regular Expression Denial of Service (ReDoS) attack. If an attacker can put a lot of JSX elements into `<blockquote>` tag _with including multibyte characters_, an internal regular expression for escaping characters may consume an excessive amount of computing resources. v4.5.1 passes the test against ASCII characters but misses the case of multibyte characters. jsx-slack v4.5.2 has updated regular expressions for escaping blockquote characters to prevent catastrophic backtracking. It is also including an updated test case to confirm rendering multiple tags in `<blockquote>` with multibyte characters.	2021-12-20	not yet calculated	CVE-2021-43843 CONFIRM MISC MISC MISC
kataras -- iris	This affects all versions of package github.com/kataras/iris; all versions of package github.com/kataras/iris/v12. The unsafe handling of file names during upload using UploadFormFiles method may enable attackers to write to arbitrary locations outside the designated target folder.	2021-12-24	not yet calculated	CVE-2021-23772 CONFIRM CONFIRM CONFIRM
lantronix -- premierwave	A specially-crafted HTTP request can lead to arbitrary command execution in EC keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21875 MISC
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager Diagnostics: Traceroute functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21872 MISC
lantronix -- premierwave	Specially-crafted HTTP requests can lead to arbitrary command execution in PUT requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21876 MISC
lantronix -- premierwave	Specially-crafted HTTP requests can lead to arbitrary command execution in “GET” requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21877 MISC
lantronix -- premierwave	A specially-crafted HTTP request can lead to arbitrary command execution in DSA keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21874 MISC
lantronix -- premierwave	A specially-crafted HTTP request can lead to arbitrary command execution in RSA keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21873 MISC
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager Wireless Network Scanner functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21881 MISC
lantronix -- premierwave	A stack-based buffer overflow vulnerability exists in the Web Manager SslGenerateCSR functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21887 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager SslGenerateCSR functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21884 MISC
lantronix -- premierwave	A stack-based buffer overflow vulnerability exists in the Web Manager FsUnmount functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21892 MISC
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager SslGenerateCertificate functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21888 MISC
lantronix -- premierwave	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletefile). An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21891 MISC
lantronix -- premierwave	A local file inclusion vulnerability exists in the Web Manager Applications and FsBrowse functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted series of HTTP requests can lead to local file inclusion. An attacker can make a series of authenticated HTTP requests to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21878 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FsMove functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21885 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FSBrowsePage functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to information disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21886 MISC
lantronix -- premierwave	A stack-based buffer overflow vulnerability exists in the Web Manager Ping functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21889 MISC
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager Diagnostics: Ping functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21883 MISC
lantronix -- premierwave	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletedir). An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21890 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary file overwrite FsTFtp file disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21894 MISC
lantronix -- premierwave	An OS command injection vulnerability exists in the Web Manager FsUnmount functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21882 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to FsTFtp file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21895 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FsCopyFile functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21880 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary file deletion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21896 MISC
lantronix -- premierwave	A directory traversal vulnerability exists in the Web Manager File Upload functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-12-22	not yet calculated	CVE-2021-21879 MISC
lib/cmd.js -- lib/cmd.js	lib/cmd.js in the node-windows package before 1.0.0-beta.6 for Node.js allows command injection via the PID parameter.	2021-12-22	not yet calculated	CVE-2021-45459 MISC MISC
linux -- linux_kernel	In the IPv4 implementation in the Linux kernel before 5.12.4, net/ipv4/route.c has an information leak because the hash table is very small.	2021-12-25	not yet calculated	CVE-2021-45486 MISC MISC MISC
linux -- linux_kernel	A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11. This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a shared memory object.	2021-12-22	not yet calculated	CVE-2021-44733 MISC MISC
linux -- linux_kernel	In __f2fs_setxattr in fs/f2fs/xattr.c in the Linux kernel through 5.15.11, there is an out-of-bounds memory access when an inode has an invalid last xattr entry.	2021-12-23	not yet calculated	CVE-2021-45469 MISC MISC MLIST
linux -- linux_kernel	In the IPv6 implementation in the Linux kernel before 5.13.3, net/ipv6/output_core.c has an information leak because of certain use of a hash table which, although big, doesn't properly consider that IPv6-based attackers can typically choose among many IPv6 source addresses.	2021-12-25	not yet calculated	CVE-2021-45485 MISC MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.15.11. There is a memory leak in the __rds_conn_create() function in net/rds/connection.c in a certain combination of circumstances.	2021-12-24	not yet calculated	CVE-2021-45480 MISC MISC
mart_developers_inc -- iorder	An HTML Injection Vulnerability in iOrder 1.0 allows the remote attacker to execute Malicious HTML codes via the signup form	2021-12-20	not yet calculated	CVE-2021-43441 MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, XSS can occur in Wikibase because an external identifier property can have a URL format that includes a $1 formatter substitution marker, and the javascript: URL scheme (among others) can be used.	2021-12-24	not yet calculated	CVE-2021-45472 MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, the Special:ImportFile URI (aka FileImporter) allows XSS, as demonstrated by the clientUrl parameter.	2021-12-24	not yet calculated	CVE-2021-45474 MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, Wikibase item descriptions allow XSS, which is triggered upon a visit to an action=info URL (aka a page-information sidebar).	2021-12-24	not yet calculated	CVE-2021-45473 MISC MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. It is possible to use action=edit&undo= followed by action=mcrundo and action=mcrrestore to view private pages on a private wiki that has at least one page set in $wgWhitelistRead.	2021-12-20	not yet calculated	CVE-2021-44858 CONFIRM MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, blocked IP addresses are allowed to edit EntitySchema items.	2021-12-24	not yet calculated	CVE-2021-45471 MISC MISC MISC
mesa_labs -- amegaview	Mesa Labs AmegaView Versions 3.0 uses default cookies that could be set to bypass authentication to the web application, which may allow an attacker to gain access.	2021-12-21	not yet calculated	CVE-2021-27453 CONFIRM
mesa_labs -- amegaview	Mesa Labs AmegaView Versions 3.0 and prior's passcode is generated by an easily reversible algorithm, which may allow an attacker to gain access to the device.	2021-12-21	not yet calculated	CVE-2021-27451 CONFIRM
mesa_labs -- amegaview	Mesa Labs AmegaView version 3.0 is vulnerable to a command injection, which may allow an attacker to remotely execute arbitrary code.	2021-12-21	not yet calculated	CVE-2021-27447 MISC
mesa_labs -- amegaview	Mesa Labs AmegaView Versions 3.0 and prior has insecure file permissions that could be exploited to escalate privileges on the device.	2021-12-21	not yet calculated	CVE-2021-27445 CONFIRM
mesa_labs -- amegaview	Mesa Labs AmegaView Versions 3.0 and prior has a command injection vulnerability that can be exploited to execute commands in the web server.	2021-12-21	not yet calculated	CVE-2021-27449 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
msedgeredirect -- msedgeredirect	MSEdgeRedirect is a tool to redirect news, search, widgets, weather, and more to a user's default browser. MSEdgeRedirect versions before 0.5.0.1 are vulnerable to Remote Code Execution via specifically crafted URLs. This vulnerability requires user interaction and the acceptance of a prompt. With how MSEdgeRedirect is coded, parameters are impossible to pass to any launched file. However, there are two possible scenarios in which an attacker can do more than a minor annoyance. In Scenario 1 (confirmed), a user visits an attacker controlled webpage; the user is prompted with, and downloads, an executable payload; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and RCE executes the payload the user previously downloaded, if the download path is successfully guessed. In Scenario 2 (not yet confirmed), a user visits an attacked controlled webpage; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and a payload on a remote, attacker controlled, SMB server is executed. The issue was found in the _DecodeAndRun() function, in which I incorrectly assumed _WinAPI_UrlIs() would only accept web resources. Unfortunately, file:/// passes the default _WinAPI_UrlIs check(). File paths are now directly checked for and must fail. There is no currently known exploitation of this vulnerability in the wild. A patched version, 0.5.0.1, has been released that checks for and denies these crafted URLs. There are no workarounds for this issue. Users are advised not to accept any unexpected prompts from web pages.	2021-12-20	not yet calculated	CVE-2021-43844 CONFIRM MISC
myscada -- mypro	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the password can be specified, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	2021-12-23	not yet calculated	CVE-2021-23198 MISC
myscada -- mypro	An additional, nondocumented administrative account exists in mySCADA myPRO Versions 8.20.0 and prior that is not exposed through the web interface, which cannot be deleted or changed through the regular web interface.	2021-12-23	not yet calculated	CVE-2021-43987 MISC
myscada -- mypro	mySCADA myPRO: Versions 8.20.0 and prior has a vulnerable debug interface which includes a ping utility, which may allow an attacker to inject arbitrary operating system commands.	2021-12-23	not yet calculated	CVE-2021-44453 MISC
myscada -- mypro	mySCADA myPRO Versions 8.20.0 and prior stores passwords using MD5, which may allow an attacker to crack the previously retrieved password hashes.	2021-12-23	not yet calculated	CVE-2021-43989 MISC
myscada -- mypro	mySCADA myPRO: Versions 8.20.0 and prior has a feature to send emails, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	2021-12-23	not yet calculated	CVE-2021-43981 MISC
myscada -- mypro	An unauthenticated remote attacker can access mySCADA myPRO Versions 8.20.0 and prior without any form of authentication or authorization.	2021-12-23	not yet calculated	CVE-2021-43985 MISC
myscada -- mypro	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the firmware can be updated, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	2021-12-23	not yet calculated	CVE-2021-43984 MISC
myscada -- mypro	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the API password can be specified, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	2021-12-23	not yet calculated	CVE-2021-22657 MISC
nasm -- nasm	A Null Pointer Dereference vulnerability existfs in nasm 2.16rc0 via asm/preproc.c.	2021-12-22	not yet calculated	CVE-2021-45256 MISC
nasm -- nasm	An infinite loop vulnerability exists in nasm 2.16rc0 via the gpaste_tokens function.	2021-12-22	not yet calculated	CVE-2021-45257 MISC
netapp -- storagegrid	StorageGRID (formerly StorageGRID Webscale) versions 11.5 prior to 11.5.0.5 are susceptible to a vulnerability which may allow an administrative user to escalate their privileges and modify settings in SANtricity System Manager.	2021-12-23	not yet calculated	CVE-2021-27006 MISC
netapp -- virtual_desktop_service	NetApp Virtual Desktop Service (VDS) when used with an HTML5 gateway is susceptible to a vulnerability which when successfully exploited could allow an unauthenticated attacker to takeover a Remote Desktop Session.	2021-12-23	not yet calculated	CVE-2021-27007 MISC
netbsd -- netbsd	In NetBSD through 9.2, the IPv4 ID generation algorithm does not use appropriate cryptographic measures.	2021-12-25	not yet calculated	CVE-2021-45487 MISC MISC
netbsd -- netbsd	In NetBSD through 9.2, the IPv6 Flow Label generation algorithm employs a weak cryptographic PRNG.	2021-12-25	not yet calculated	CVE-2021-45489 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netbsd -- netbsd	In NetBSD through 9.2, there is an information leak in the TCP ISN (ISS) generation algorithm.	2021-12-25	not yet calculated	CVE-2021-45488 MISC MISC
netbsd -- netbsd	In NetBSD through 9.2, the IPv6 fragment ID generation algorithm employs a weak cryptographic PRNG.	2021-12-25	not yet calculated	CVE-2021-45484 MISC MISC
nltk -- nltk	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. Versions prior to 3.6.5 are vulnerable to regular expression denial of service (ReDoS) attacks. The vulnerability is present in PunktSentenceTokenizer, sent_tokenize and word_tokenize. Any users of this class, or these two functions, are vulnerable to the ReDoS attack. In short, a specifically crafted long input to any of these vulnerable functions will cause them to take a significant amount of execution time. If your program relies on any of the vulnerable functions for tokenizing unpredictable user input, then we would strongly recommend upgrading to a version of NLTK without the vulnerability. For users unable to upgrade the execution time can be bounded by limiting the maximum length of an input to any of the vulnerable functions. Our recommendation is to implement such a limit.	2021-12-23	not yet calculated	CVE-2021-43854 MISC MISC CONFIRM MISC
nvidia -- geforce	NVIDIA GeForce Experience contains a vulnerability in user authorization, where GameStream does not correctly apply individual user access controls for users on the same device, which, with user intervention, may lead to escalation of privileges, information disclosure, data tampering, and denial of service, affecting other resources beyond the intended security authority of GameStream.	2021-12-23	not yet calculated	CVE-2021-23175 CONFIRM
online_enrollment_management_system_-_online_enrollment_management_system	The id parameter from Online Enrollment Management System 1.0 system appears to be vulnerable to SQL injection attacks. A crafted payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can retrieve sensitive information for all users of this system.	2021-12-23	not yet calculated	CVE-2021-44599 MISC
open5gs -- open5gs	In Open5GS 2.4.0, a crafted packet from UE can crash SGW-U/UPF.	2021-12-23	not yet calculated	CVE-2021-45462 MISC
open_design_alliance -- drawings_explorer	An out-of-bounds read vulnerability exists when reading a BMP file using Open Design Alliance (ODA) Drawings Explorer before 2022.12. The specific issue exists after loading BMP files. Unchecked input data from a crafted BMP file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	2021-12-21	not yet calculated	CVE-2021-44423 MISC
open_design_alliance -- drawings_sdk	An Improper Input Validation Vulnerability exists when reading a BMP file using Open Design Alliance Drawings SDK before 2022.12. Crafted data in a BMP file can trigger a write operation past the end of an allocated buffer, or lead to a heap-based buffer overflow. An attacker can leverage this vulnerability to execute code in the context of the current process.	2021-12-21	not yet calculated	CVE-2021-44422 MISC
opendesign -- drawings_sdk	An out-of-bounds read vulnerability exists when reading a TGA file using Open Design Alliance Drawings SDK before 2022.12. The specific issue exists after loading TGA files. An unchecked input data from a crafted TGA file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	2021-12-21	not yet calculated	CVE-2021-44859 MISC
opendesign -- drawings_sdk	An out-of-bounds read vulnerability exists when reading a TIF file using Open Design Alliance Drawings SDK before 2022.12. The specific issue exists after loading TIF files. An unchecked input data from a crafted TIF file leads to an out-of-bounds read. An attacker can leverage this vulnerability to execute code in the context of the current process.	2021-12-21	not yet calculated	CVE-2021-44860 MISC
opmantak -- open-audit	An issue was discovered in Opmantek Open-AudIT after 3.5.0. Without authentication, a vulnerability in code_igniter/application/controllers/util.php allows an attacker perform command execution without echoes.	2021-12-22	not yet calculated	CVE-2021-40612 MISC MISC
opmantek -- open-auditit_community	Opmantek Open-AudIT Community 4.2.0 (Fixed in 4.3.0) is affected by a Cross Site Scripting (XSS) vulnerability. If a bad value is passed to the routine via a URL, malicious JavaScript code can be executed in the victim's browser.	2021-12-20	not yet calculated	CVE-2021-44916 MISC MISC MISC
parse-link-header -- parse-link-header	The package parse-link-header before 2.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the checkHeader function.	2021-12-24	not yet calculated	CVE-2021-23490 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pimcore -- pimcore	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-21	not yet calculated	CVE-2021-4139 MISC CONFIRM
pjsip -- pjsip	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In affected versions if the incoming RTCP BYE message contains a reason's length, this declared length is not checked against the actual received packet size, potentially resulting in an out-of-bound read access. This issue affects all users that use PJMEDIA and RTCP. A malicious actor can send a RTCP BYE message with an invalid reason length. Users are advised to upgrade as soon as possible. There are no known workarounds.	2021-12-22	not yet calculated	CVE-2021-43804 CONFIRM MISC
pjsip --pjsip	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In affected versions if the incoming STUN message contains an ERROR-CODE attribute, the header length is not checked before performing a subtraction operation, potentially resulting in an integer underflow scenario. This issue affects all users that use STUN. A malicious actor located within the victim's network may forge and send a specially crafted UDP (STUN) message that could remotely execute arbitrary code on the victim's machine. Users are advised to upgrade as soon as possible. There are no known workarounds.	2021-12-22	not yet calculated	CVE-2021-37706 CONFIRM MISC
podman -- podman	A flaw was found in podman. The `podman machine` function (used to create and manage Podman virtual machine containing a Podman process) spawns a `gvproxy` process on the host system. The `gvproxy` API is accessible on port 7777 on all IP addresses on the host. If that port is open on the host's firewall, an attacker can potentially use the `gvproxy` API to forward ports on the host to ports in the VM, making private services on the VM accessible to the network. This issue could be also used to interrupt the host's services by forwarding all ports to the VM.	2021-12-23	not yet calculated	CVE-2021-4024 MISC MISC
prestashop -- prestashop	PrestaShop before 1.5.2 allows XSS via the "<object data='data:text/html" substring in the message field.	2021-12-21	not yet calculated	CVE-2012-20001 MISC
privoxy -- privoxy	An XSS vulnerability was found in Privoxy which was fixed in cgi_error_no_template() by encode the template name when Privoxy is configured to servce the user-manual itself.	2021-12-23	not yet calculated	CVE-2021-44543 MISC MISC
privoxy -- privoxy	A memory leak vulnerability was found in Privoxy when handling errors.	2021-12-23	not yet calculated	CVE-2021-44542 MISC MISC
privoxy -- privoxy	A vulnerability was found in Privoxy which was fixed in process_encrypted_request_headers() by freeing header memory when failing to get the request destination.	2021-12-23	not yet calculated	CVE-2021-44541 MISC MISC
privoxy -- privoxy	A vulnerability was found in Privoxy which was fixed in get_url_spec_param() by freeing memory of compiled pattern spec before bailing.	2021-12-23	not yet calculated	CVE-2021-44540 MISC MISC
projectworlds -- hospital_management_system	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via multiple parameters in admin_home.php.	2021-12-22	not yet calculated	CVE-2021-43629 MISC MISC
projectworlds -- hospital_management_system	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via the appointment_no parameter in payment.php.	2021-12-22	not yet calculated	CVE-2021-43631 MISC MISC
projectworlds -- hospital_management_system	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via the email parameter in hms-staff.php.	2021-12-22	not yet calculated	CVE-2021-43628 MISC MISC
projectworlds -- hospital_management_system	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via multiple parameters in add_patient.php. As a result, an authenticated malicious user can compromise the databases system and in some cases leverage this vulnerability to get remote code execution on the remote web server.	2021-12-22	not yet calculated	CVE-2021-43630 MISC MISC
projectworlds -- online_book_store	In ProjectWorlds Online Book Store PHP 1.0 a CSRF vulnerability in admin_delete.php allows a remote attacker to delete any book.	2021-12-22	not yet calculated	CVE-2021-43156 MISC
projectworlds -- online_book_store	Projectsworlds Online Shopping System PHP 1.0 is vulnerable to SQL injection via the id parameter in cart_remove.php.	2021-12-22	not yet calculated	CVE-2021-43157 MISC MISC
projectworlds -- online_book_store	Projectsworlds Online Book Store PHP v1.0 is vulnerable to SQL injection via the "bookisbn" parameter in cart.php.	2021-12-22	not yet calculated	CVE-2021-43155 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds -- online_book_store	In ProjectWorlds Online Shopping System PHP 1.0, a CSRF vulnerability in cart_remove.php allows a remote attacker to remove any product in the customer's cart.	2021-12-22	not yet calculated	CVE-2021-43158 MISC MISC
pytorch_lightning -- pytorch_lightning	pytorch-lightning is vulnerable to Deserialization of Untrusted Data	2021-12-23	not yet calculated	CVE-2021-4118 MISC CONFIRM
quest -- kace_desktop_authority	Quest KACE Desktop Authority before 11.2 allows XSS because it does not prevent untrusted HTML from reaching the jQuery.htmlPrefilter method of jQuery.	2021-12-22	not yet calculated	CVE-2021-44030 CONFIRM
quest -- kace_desktop_authority	An issue was discovered in Quest KACE Desktop Authority before 11.2. /dacomponentui/profiles/profileitems/outlooksettings/Insertimage.aspx contains a vulnerability that could allow pre-authentication remote code execution. An attacker could upload a .ASP file to reside at /images/{GUID}/{filename}.	2021-12-22	not yet calculated	CVE-2021-44031 MISC
quest -- kace_desktop_authority	An issue was discovered in Quest KACE Desktop Authority before 11.2. This vulnerability allows attackers to execute remote code through a deserialization exploitation in the RadAsyncUpload function of ASP.NET AJAX. An attacker can leverage this vulnerability when the encryption keys are known (due to the presence of CVE-2017-11317, CVE-2017-11357, or other means). A default setting for the type whitelisting feature in more current versions of ASP.NET AJAX prevents exploitation.	2021-12-22	not yet calculated	CVE-2021-44029 MISC
quest -- kace_desktop_authority	XXE can occur in Quest KACE Desktop Authority before 11.2 because the log4net configuration file might be controlled by an attacker, a related issue to CVE-2018-1285.	2021-12-22	not yet calculated	CVE-2021-44028 MISC
realtek -- rtl8195am_device	A stack buffer overflow was discovered on Realtek RTL8195AM device before 2.0.10, it exists in the client code when an attacker sends a big size Authentication challenge text in WEP security.	2021-12-22	not yet calculated	CVE-2021-39306 MISC MISC
rockoa -- rockoa	A cross-site request forgery (CSRF) in Rockoa v1.9.8 allows an authenticated attacker to arbitrarily add an administrator account.	2021-12-22	not yet calculated	CVE-2020-20593 MISC MISC
samsung -- printers	The SyncThru Web Service on Samsung SCX-6x55X printers allows an attacker to gain access to a list of SMB users and cleartext passwords by reading the HTML source code. Authentication is not required.	2021-12-20	not yet calculated	CVE-2021-42913 MISC MISC
simple -- cold_storage_management_system	The id parameter in view_storage.php from Simple Cold Storage Management System 1.0 appears to be vulnerable to SQL injection attacks. A payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.	2021-12-21	not yet calculated	CVE-2021-45253 MISC
simple -- forum_discussion_system	Multiple SQL injection vulnerabilities are found on Simple Forum-Discussion System 1.0 For example on three applications which are manage_topic.php, manage_user.php, and ajax.php. The attacker can be retrieving all information from the database of this system by using this vulnerability.	2021-12-21	not yet calculated	CVE-2021-45252 MISC
simple_online_mens_salon_management_system - - simple_online_mens_salon_management_system	The password parameter on Simple Online Mens Salon Management System (MSMS) 1.0 appears to be vulnerable to SQL injection attacks through the password parameter. The predictive tests of this application interacted with that domain, indicating that the injected SQL query was executed. The attacker can retrieve all authentication and information about the users of this system.	2021-12-23	not yet calculated	CVE-2021-44600 MISC
solarwinds -- orion	It has been reported that any Orion user, e.g. guest accounts can query the Orion.UserSettings entity and enumerate users and their basic settings.	2021-12-20	not yet calculated	CVE-2021-35248 MISC MISC MISC
solarwinds -- orion	The "Log alert to a file" action within action management enables any Orion Platform user with Orion alert management rights to write to any file. An attacker with Orion alert management rights could use this vulnerability to perform an unrestricted file upload causing a remote code execution.	2021-12-20	not yet calculated	CVE-2021-35244 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- orion	Numerous exposed dangerous functions within Orion Core has allows for read-only SQL injection leading to privileged escalation. An attacker with low-user privileges may steal password hashes and password salt information.	2021-12-20	not yet calculated	CVE-2021-35234 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
solarwinds -- web_help_desk	The HTTP PUT and DELETE methods were enabled in the Web Help Desk web server (12.7.6 and earlier), allowing users to execute dangerous HTTP requests. The HTTP PUT method is normally used to upload data that is saved on the server with a user-supplied URL. While the DELETE method requests that the origin server removes the association between the target resource and its current functionality. Improper use of these methods may lead to a loss of integrity.	2021-12-23	not yet calculated	CVE-2021-35243 MISC
solidusio -- solidus	`solidus_frontend` is the cart and storefront for the Solidus e-commerce project. Versions of `solidus_frontend` prior to 3.1.5, 3.0.5, and 2.11.14 contain a cross-site request forgery (CSRF) vulnerability that allows a malicious site to add an item to the user's cart without their knowledge. Versions 3.1.5, 3.0.5, and 2.11.14 contain a patch for this issue. The patch adds CSRF token verification to the "Add to cart" action. Adding forgery protection to a form that missed it can have some side effects. Other CSRF protection strategies as well as a workaround involving modifcation to config/application.rb` are available. More details on these mitigations are available in the GitHub Security Advisory.	2021-12-20	not yet calculated	CVE-2021-43846 MISC MISC CONFIRM
sonicwall -- sma100_series	A vulnerability in SonicWall SMA100 password change API allows a remote unauthenticated attacker to perform SMA100 username enumeration based on the server responses. This vulnerability impacts 10.2.1.2-24sv, 10.2.0.8-37sv and earlier 10.x versions.	2021-12-23	not yet calculated	CVE-2021-20049 CONFIRM
sonicwall -- sma100_series	An Improper Access Control Vulnerability in the SMA100 series leads to multiple restricted management APIs being accessible without a user login, potentially exposing configuration meta-data.	2021-12-23	not yet calculated	CVE-2021-20050 CONFIRM
sourcecodetester -- engineers_online_portal	In sourcecodetester Engineers Online Portal as of 10-21-21, an attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways. Very often multiple websites are hosted on the same IP address. This is where the Host Header comes in. This header specifies which website should process the HTTP request. The web server uses the value of this header to dispatch the request to the specified website. Each website hosted on the same IP address is called a virtual host. And It's possible to send requests with arbitrary Host Headers to the first virtual host.	2021-12-20	not yet calculated	CVE-2021-43437 MISC MISC
sssd -- sssd	A flaw was found in SSSD, where the sssctl command was vulnerable to shell command injection via the logs-fetch and cache-expire subcommands. This flaw allows an attacker to trick the root user into running a specially crafted sssctl command, such as via sudo, to gain root access. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-12-23	not yet calculated	CVE-2021-3621 MISC MISC
starcharge -- multiple_products	Certain Starcharge products are affected by Improper Input Validation. The affected products include: Nova 360 Cabinet <= 1.3.0.0.7b102 - Fixed: Beta1.3.0.1.0 and Titan 180 Premium <= 1.3.0.0.6 - Fixed: 1.3.0.0.9.	2021-12-22	not yet calculated	CVE-2021-45419 MISC MISC MISC
starcharge -- multiple_products	Certain Starcharge products are vulnerable to Directory Traversal via main.cgi. The affected products include: Nova 360 Cabinet <=1.3.0.0.6 - Fixed: 1.3.0.0.9 and Titan 180 Premium <=1.3.0.0.7b102 - Fixed: Beta1.3.0.1.0.	2021-12-22	not yet calculated	CVE-2021-45418 MISC MISC MISC
stormshield -- stormshield_endpoint_security	Stormshield Endpoint Security from 2.1.0 to 2.1.1 has Incorrect Access Control.	2021-12-21	not yet calculated	CVE-2021-45091 MISC
stormshield -- stormshield_endpoint_security	Stormshield Endpoint Security before 2.1.2 allows remote code execution.	2021-12-21	not yet calculated	CVE-2021-45090 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stormshield -- stormshield_endpoint_security	Stormshield Endpoint Security 2.x before 2.1.2 has Incorrect Access Control.	2021-12-21	not yet calculated	CVE-2021-45089 MISC
thales -- safenet_agent	A user of a machine protected by SafeNet Agent for Windows Logon may leverage weak entropy to access the encrypted credentials of any or all the users on that machine.	2021-12-20	not yet calculated	CVE-2021-42138 MISC MISC MISC
thales -- sentinel_protection_installer	Improper Access Control in Thales Sentinel Protection Installer could allow a local user to escalate privileges.	2021-12-20	not yet calculated	CVE-2021-42808 MISC
thales -- sentinel_protection_installer	Improper Access Control of Dynamically-Managed Code Resources (DLL) in Thales Sentinel Protection Installer could allow the execution of arbitrary code.	2021-12-20	not yet calculated	CVE-2021-42809 MISC
theforeman -- foreman	A server side remote code execution vulnerability was found in Foreman project. A authenticated attacker could use Sendmail configuration options to overwrite the defaults and perform command injection. The highest threat from this vulnerability is to confidentiality, integrity and availability of system. Fixed releases are 2.4.1, 2.5.1, 3.0.0.	2021-12-23	not yet calculated	CVE-2021-3584 MISC MISC MISC
thinfinity -- virtualui	Thinfinity VirtualUI before 3.0 allows a malicious actor to enumerate users registered in the OS (Windows) through the /changePassword URI. By accessing the vector, an attacker can determine if a username exists thanks to the message returned; it can be presented in different languages according to the configuration of VirtualUI. Common users are administrator, admin, guest and krgtbt.	2021-12-20	not yet calculated	CVE-2021-44554 MISC
thinkcmf -- thinkcmf	An issue in ThinkCMF X2.2.2 and below allows attackers to execute arbitrary code via a crafted packet.	2021-12-22	not yet calculated	CVE-2020-20601 MISC
tp-link -- ax10v1	A misconfiguration in HTTP/1.0 and HTTP/1.1 of the web interface in TP-Link AX10v1 before V1_211117 allows a remote unauthenticated attacker to send a specially crafted HTTP request and receive a misconfigured HTTP/0.9 response, potentially leading into a cache poisoning attack.	2021-12-17	not yet calculated	CVE-2021-41451 MISC MISC MISC
tp-link -- wifi_router	TP-Link wifi router TL-WR802N V4(JP), with firmware version prior to 211202, is vulnerable to OS command injection.	2021-12-23	not yet calculated	CVE-2021-4144 JVN CONFIRM
uti_mutual_fund_android_application - - uti_mutual_fund_android_application	An issue was discovered in UTI Mutual fund Android application 5.4.18 and prior, allows attackers to brute force enumeration of usernames determined by the error message returned after invalid credentials are attempted.	2021-12-23	not yet calculated	CVE-2020-35398 MISC MISC
video_sharing_website -- video_sharing_website	The email parameter from ajax.php of Video Sharing Website 1.0 appears to be vulnerable to SQL injection attacks. A payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.	2021-12-21	not yet calculated	CVE-2021-45255 MISC
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2021-12-19	not yet calculated	CVE-2021-4136 CONFIRM MISC
vim -- vim	vim is vulnerable to Out-of-bounds Read	2021-12-25	not yet calculated	CVE-2021-4166 CONFIRM MISC
vmware -- workspace_one_access	VMware Workspace ONE Access 21.08, 20.10.0.1, and 20.10 and Identity Manager 3.3.5, 3.3.4, and 3.3.3 contain an SSRF vulnerability. A malicious actor with network access may be able to make HTTP requests to arbitrary origins and read the full response.	2021-12-20	not yet calculated	CVE-2021-22056 MISC
vmware -- workspace_one_access	VMware Workspace ONE Access 21.08, 20.10.0.1, and 20.10 contain an authentication bypass vulnerability. A malicious actor, who has successfully provided first-factor authentication, may be able to obtain second-factor authentication provided by VMware Verify.	2021-12-20	not yet calculated	CVE-2021-22057 MISC
webassembly -- binaryen	A Denial of Service vulnerability exits in Binaryen 103 due to an assertion abort in wasm::handle_unreachable.	2021-12-21	not yet calculated	CVE-2021-45290 MISC
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 103 due to an Invalid memory address dereference in wasm::WasmBinaryBuilder::visitLet.	2021-12-21	not yet calculated	CVE-2021-45293 MISC
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::Frame::page, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45483 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::ContainerNode::firstChild, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45482 MISC
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is incorrect memory allocation in WebCore::ImageBufferCairoImageSurfaceBackend::create, leading to a segmentation violation and application crash, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45481 MISC
wordpress -- directorist	The Directorist WordPress plugin before 7.0.6.2 was vulnerable to Cross-Site Request Forgery to Remote File Upload leading to arbitrary PHP shell uploads in the wp-content/plugins directory.	2021-12-21	not yet calculated	CVE-2021-24981 MISC MISC
wordpress -- logo_carousel	The Logo Carousel WordPress plugin before 3.4.2 allows users with a role as low as Contributor to duplicate and view arbitrary private posts made by other users via the Carousel Duplication feature	2021-12-21	not yet calculated	CVE-2021-24739 MISC
wordpress -- logo_carousel	The Logo Carousel WordPress plugin before 3.4.2 does not validate and escape the "Logo Margin" carousel option, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	2021-12-21	not yet calculated	CVE-2021-24738 MISC
wordpress -- sportspress	The SportsPress WordPress plugin before 2.7.9 does not sanitise and escape its match_day parameter before outputting back in the Events backend page, leading to a Reflected Cross-Site Scripting issue	2021-12-21	not yet calculated	CVE-2021-24578 MISC
wordpress -- wcfm_marketplace	The wcfm_ajax_controller AJAX action of the WCFM Marketplace WordPress plugin before 3.4.12, available to unauthenticated and authenticated user, does not properly sanitise multiple parameters before using them in SQL statements, leading to SQL injections	2021-12-21	not yet calculated	CVE-2021-24849 MISC
wordpress -- wordpress	The get_query() function of the Ni WooCommerce Custom Order Status WordPress plugin before 1.9.7, used by the niwoocos_ajax AJAX action, available to all authenticated users, does not properly sanitise the sort parameter before using it in a SQL statement, leading to an SQL injection, exploitable by any authenticated users, such as subscriber	2021-12-21	not yet calculated	CVE-2021-24846 MISC
wordpress -- wordpress	The Contact Form, Drag and Drop Form Builder for WordPress plugin before 1.8.0 does not escape the status parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue	2021-12-21	not yet calculated	CVE-2021-24907 MISC
wordpress -- wordpress	The Popups, Welcome Bar, Optins and Lead Generation Plugin WordPress plugin before 2.0.5 does not sanitise and escape the message_id parameter of the get_message_action_row AJAX action before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue	2021-12-21	not yet calculated	CVE-2021-24941 MISC
wordpress -- wordpress	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.8.7 does not sanitise and escape the b2sShowByDate parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue	2021-12-21	not yet calculated	CVE-2021-24956 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability leading to Cross-Site Scripting (XSS) discovered in tarteaucitron.js – Cookies legislation & GDPR WordPress plugin (versions <= 1.5.4), vulnerable parameters "tarteaucitronEmail" and "tarteaucitronPass".	2021-12-20	not yet calculated	CVE-2021-36887 CONFIRM MISC
wordpress wp_visitor_statistics	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 4.8 does not properly sanitise and escape the refUrl in the refDetails AJAX action, available to any authenticated user, which could allow users with a role as low as subscriber to perform SQL injection attacks	2021-12-21	not yet calculated	CVE-2021-24750 MISC CONFIRM
wuzhi_cms -- wuzhi_cms	A cross-site scripting (XSS) vulnerability in the system bulletin component of WUZHI CMS v4.1.0 allows attackers to steal the admin's cookie.	2021-12-21	not yet calculated	CVE-2020-19770 MISC
zohocorp -- manageengine_log360	Zoho ManageEngine ServiceDesk Plus before 12003 allows authentication bypass in certain admin configurations.	2021-12-23	not yet calculated	CVE-2021-44526 MISC
zohocorp -- manageengine_log360	Zoho ManageEngine Access Manager Plus before 4203 allows anyone to view a few data elements (e.g., access control details) and modify a few aspects of the application state.	2021-12-20	not yet calculated	CVE-2021-44676 CONFIRM MISC
zohocorp -- manageengine_log360	Zoho ManageEngine ServiceDesk Plus MSP before 10.5 Build 10534 is vulnerable to unauthenticated remote code execution due to a filter bypass in which authentication is not required.	2021-12-20	not yet calculated	CVE-2021-44675 CONFIRM
zohocorp -- manageengine_log360	Zoho ManageEngine PAM360 before build 5303 allows attackers to modify a few aspects of application state because of a filter bypass in which authentication is not required.	2021-12-20	not yet calculated	CVE-2021-44525 CONFIRM

Back to top